11-1126

To Be Argued By:
JOSEPH P. FACCIPONTI

United States Court of Appeals

FOR THE SECOND CIRCUIT

Docket No. 11-1126

UNITED STATES OF AMERICA,

Appellee,

—v.—

SERGEY ALEYNIKOV,

Defendant-Appellant.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

BRIEF FOR THE UNITED STATES OF AMERICA

PREET BHARARA,
United States Attorney for the Southern District of New York,
Attorney for the United States of America.

JOSEPH P. FACCIPONTI,
JUSTIN S. WEDDLE,
Assistant United States Attorneys,
Of Counsel.

TABLE OF CONTENTS

PAGE

TABLE OF AUTHORITIES

Cases:

PAGE

PAGE

PAGE

PAGE

United States Court of Appeals

FOR THE SECOND CIRCUIT

Docket No. 11-1126

UNITED STATES OF AMERICA,

Appellee,

-v.-

SERGEY ALEYNIKOV,

Defendant-Appellant.

BRIEF FOR THE UNITED STATES OF AMERICA

Preliminary Statement

Sergey Aleynikov appeals from a judgment of conviction entered on March 23, 2011, in the United States District Court for the Southern District of New York, following a two-week trial before the Honorable Denise L. Cote, United States District Judge, and a jury.

Indictment 10 Cr. 96 (DLC) was filed on February 11, 2010, in three counts. Count One charged Aleynikov with theft of trade secrets, in violation of Title 18, United States Code, Section 1832; Count Two charged Aleynikov with interstate transportation of stolen property, in violation of

Title 18, United States Code, Section 2314; and Count Three charged Aleynikov with unauthorized computer access, in violation of Title 18, United States Code, Section 1030.

On September 3, 2010, the District Court issued an opinion and order denying Aleynikov's motion to dismiss Count One and Count Two for failure to state claims, but granting his motion to dismiss Count Three. *See United States* v. *Aleynikov*, 737 F. Supp. 2d 173 (S.D.N.Y. 2010).

Trial commenced on November 29, 2010 and ended on December 10, 2010, when the jury returned a guilty verdict on both of the remaining counts of the Indictment.

On March 16, 2011, the District Court denied Aleynikov's post-trial motions in a written order and opinion. *See United States* v. *Aleynikov*, No. 10 Cr. 96 (DLC), 2011 WL 939754 (S.D.N.Y. Mar. 16, 2011).

On March 18, 2011, Judge Cote sentenced Aleynikov to a term of 97 months' imprisonment, a term of three years' supervised release, and a fine of $12,500. Aleynikov moved for bail pending appeal, which Judge Cote denied in a written opinion and order. *See United States* v. *Aleynikov*, No. 10 Cr. 96 (DLC), 2011 WL 1334850 (S.D.N.Y. Mar. 28, 2011). On May 3, 2011, after hearing oral argument, this Court denied Aleynikov's motion for bail pending appeal.

On March 23, 2011, Aleynikov filed a timely notice of appeal. Aleynikov is currently serving his sentence.

Statement of Facts

A. The Government's Case

1. Overview

Aleynikov was a computer programmer at Goldman Sachs & Co. ("Goldman"), where he worked on the code[*] to the firm's proprietary high-frequency trading ("HFT") system. (PSR ¶¶ 7, 14).[**] HFT is a form of trading in which computer programs, and not humans, make decisions to trade high volumes of securities and commodities, often in just fractions of a second. (PSR ¶¶ 8-9).

In April 2009, Aleynikov was hired by a Chicago, Illinois-based startup company, Teza Technologies LLC ("Teza"), that was seeking to develop its own HFT system. (PSR ¶ 15). On his last day of work at Goldman, without authorization and in violation of Goldman's policies, Aleynikov transferred thousands of files containing the

---

[*] As used in this case, "code" or "source code" refers to human-readable computer programming instructions written and maintained by computer programmers when developing computer programs. (Tr. 341-42).

[**] "PSR" or "Presentence Report" refers to the Presentence Investigation Report, dated March 11, 2011, prepared by the United States Probation Office ("Probation Office") in advance of Aleynikov's sentencing; "Br." refers to Aleynikov's brief on appeal; "A." refers to the appendix to Aleynikov's brief; "SPA" refers to the special appendix to Aleynikov's brief; and "Tr." refers to the trial transcript.

code to parts of Goldman's system to a computer server in Germany. (PSR ¶¶ 16-18). Aleynikov then deleted records of the transfer from Goldman's computer system. (*Id.*). Later that day and thereafter, Aleynikov downloaded the stolen code from the German server to his personal computers at his home in New Jersey. (PSR ¶ 18).

Aleynikov uploaded several of the stolen files to Teza's computer system as his own work, and brought copies of the stolen code to a meeting at Teza's Chicago offices the day before his arrest. (PSR ¶¶ 21-23).

2. Goldman's HFT System

The trial evidence[*] established that Goldman engages in HFT in financial markets in the United States and around the world (Tr. 332-40, 444-51). Goldman uses sophisticated computer systems to execute numerous trades in fractions of a second, based upon mathematical formulas that evaluate, among other things, moment--to-moment developments in the markets and data from past trades. (Tr. 332-40, 444-51, 664-79). Goldman's trading system trades on securities markets in the United States, Europe, and Asia, using computers physically located in those places. (Tr. 448).

The computer programs used to operate Goldman's trading system, like those used in any HFT system, fall

---

[*] During the trial, the District Court sealed certain exhibits and closed the courtroom during brief portions of witness testimony to protect Goldman's trade secrets. (Tr. 256-72). Aleynikov does not contest this decision on appeal.

into three basic categories. First, there are market connectivity programs that receive and process a massive volume of real-time market data and also execute trades on various markets. (Tr. 333-39, 448-49, 479-94, 670-79, 874-75). Second, there are programs that use sophisticated mathematical formulas, known as algorithms, to determine which trades the system makes, based on information from the markets. (*Id.*). Finally, there are "infrastructure" programs that ensure the quick and seamless flow of information throughout the trading system and monitor the trading system's performance. (*Id.*).

Goldman invests substantial resources in its HFT business. (Tr. 340). Goldman first acquired portions of its system by buying Hull Trading Company for approximately $500 million in 1999. (Tr. 339). Goldman then further developed and updated it with dozens of its own computer programmers. (Tr. 342-45, 449-51). In one year, the total compensation for a group of 25 of these programmers was approximately $6.875 million. (*Id.*).

Goldman also generates substantial revenue from its trading system, generating a 2009 net pretax income of approximately $300 million from just three of its groups that conduct HFT. (Tr. 449-50, 455, 982-83).

HFT is a very competitive area in which many firms are seeking to develop fast and accurate trading systems to compete for trading opportunities that might exist for only a few moments. (Tr. 335-41, 447-48, 679-711, 786-87). A competitor with Goldman's system could identify the same opportunities and diminish or eliminate Goldman's competitive advantage. (Tr. 346-48, 479-80, 533-42 , 981-82). Accordingly, like all firms that engage in HFT,

Goldman strictly guards the confidentiality of its system and does not sell or license it. (Tr. 74-75, 288-99, 346-47, 478-79, 694-95).

3. Aleynikov's Employment at Goldman

From May 2007 through June 2009, Aleynikov was employed by Goldman where he primarily worked on Goldman's HFT system's infrastructure. (Tr. 245-46, 454-63).

As part of his employment at Goldman, Aleynikov was bound by confidentiality policies and an agreement requiring him to hold the firm's confidential and proprietary information, including trade secrets, in strict confidence and to return all such information (including intellectual property created by Aleynikov) to the firm at the end of his employment. (Tr. 288-301). By early 2009, Aleynikov was the highest-paid programmer in his group with total annual compensation of $400,000. (Tr. 456-58).

4. Aleynikov's Theft of HFT Code

In April 2009, Aleynikov accepted an employment offer from Teza, a startup founded in early 2009 with the goal of developing its own HFT system. (Tr. 783-87, 805-06). Teza's founder was Mikhail Malyshev, a former head of HFT at Citadel Investment Group, a Chicago-based hedge fund ("Citadel"). (Tr. 784-85). Malyshev intended that Teza would broadly pursue "any trading strategies that would . . . be part of high frequency business" and that the scope of its trading and the markets in which it would trade would expand over time. (Tr. 787-88). Malyshev envisioned the key to Teza's success would be its ability to "react to [the] market[s] faster than anybody." (Tr. 786).

Aleynikov was to be responsible for developing the "trading platform" — i.e., the market connectivity and infrastructure — to Teza's HFT system (Tr. 794, 806-07, 879). He aggressively negotiated a compensation package at Teza ($1,150,000) that almost tripled his Goldman compensation and was second only to Teza's Chief Information Officer. (Tr. 304, 798-807, 872).

At the time, Teza was a new company without a trading system of its own or source code for such a system. (Tr. 790-91, 826, 864). On May 31, 2009, Malyshev sent Aleynikov and several others a motivational e-mail message stating that he expected Teza's new employees to develop a trading system within just six months.* (Tr. 824-27; GX 707).

Aleynikov's last day at Goldman's offices was June 5, 2009. (Tr. 463). At approximately 5:20 p.m. that day, shortly before he went to a farewell celebration with his colleagues, Aleynikov encrypted and uploaded hundreds of thousands of lines of source code for Goldman's HFT system — including source code for a "substantial part of the infrastructure and some of the algorithms and market data connectivity" — to an outside server in Germany (the "SVN Server"). (Tr. 365-66, 463, 630, 1210, 1217-18). Although Goldman attempts to block access to external

---

* By contrast, the trial evidence showed that it would take 20 computer programmers approximately 2 years to develop a competitive HFT system from scratch. (Tr. 701-02). Indeed, it takes Goldman three months to complete the software required to communicate with just one exchange. (Tr. 480).

servers to which files might be uploaded (Tr. 74-78), at that time, the SVN Server was associated with a website that was not blocked by Goldman's security firewall (Tr. 91-92, 167-68).* To facilitate this upload, Aleynikov had created a program to combine thousands of files of the source code — which had been selected for copying by Aleynikov — into two large computer files, known as "tarballs." (Tr. 188-206, 221-25; GX 224). Aleynikov's transfer of Goldman's proprietary source code to the SVN Server in Germany was not authorized by Goldman and was in violation of Goldman's policies. (Tr. 290-300, 452-64).

Aleynikov's last step was to hide his tracks by erasing records of this transfer, including records of the commands he used (known as the "bash history"), the encryption program and encryption password. (Tr. 188, 191-92, 1213-14). There is no business reason to delete the bash history; in fact, a reason to delete it is "if you don't want people to know what you've done." (Tr. 194, 220, 1373).

After returning to his home in New Jersey on the evening of June 5, 2009, Aleynikov downloaded the stolen source code from the SVN server to his home computer, and thereafter copied some of those files to his other devices. (Tr. 1210-17).

---

* The SVN Server was associated with a code-repository website named xp-dev.com that allowed computer programmers to store and manage computer code. (Tr. 1204).

In all, in his upload of June 5, 2009, Aleynikov transferred 3,639 unique files, containing more than 500,000 lines of source code, from Goldman to the SVN Server. (Tr. 1217). The files included algorithmic code; files that related to market connectivity; and infrastructure components. (Tr. 468-96, 978). Some of the code stolen by Aleynikov could operate independently of the rest of Goldman's trading system and could therefore be readily integrated into another firm's system. (Tr. 480-89). Although Aleynikov had worked on some of the code that he stole, he also stole components that he had not written or been directly involved with while at Goldman. (Tr. 482-95). One valuable component that Aleynikov stole was the model by which Goldman's trading system determines the price of stock options, known as the "TV library." (Tr. 972-83, 986-89).

In addition to the source code, Aleynikov uploaded other sensitive and confidential information regarding Goldman's trading system starting just days after he first learned about a possible job at Teza. (Tr. 510-12, 540-41, 1135-36, 1204-08). For example, on June 1, 2009 — a few days before his last day at Goldman and a day after receiving the "Let's move fast" e-mail from Malyshev (GX 707) — Aleynikov encrypted and uploaded from Goldman certain diagrams and information that he put in a file called "refm." (Tr. 1098, 1208). On June 5, 2009, Aleynikov downloaded the refm files to his personal laptop. (Tr. 1208). The refm files included proprietary evaluations of third party vendor products; evaluations of hardware and operating systems; and diagrams of Goldman's computer networks and programs. (Tr. 497-510, 1298; GX 108-A - GX 108-L).

Beginning on June 10, 2009, Aleynikov began accessing and making cosmetic changes to files that he had uploaded from Goldman — deleting, for example, information that would reveal that the files came from Goldman — and he ultimately provided some of those files to Teza by uploading them to Teza's server. (Tr. 1233-54).

On July 2, 2009, Aleynikov flew from New Jersey to Chicago, Illinois, to attend meetings at Teza's offices. (Tr. 885-87). On this trip the defendant carried with him a flash drive and a laptop computer that each contained proprietary source code stolen from Goldman. (Tr. 1136-37, 1230-31). Aleynikov returned to New Jersey on July 3, 2009, and was arrested at the airport by the Federal Bureau of Investigation ("FBI"). (Tr. 1117-18).

5. Aleynikov's Post-Arrest Statements

After his arrest, and after waiving his *Miranda* rights, Aleynikov made oral and written statements to the FBI and consented to a search of his computers and home. (Tr. 1119-34). Aleynikov admitted to the FBI that he uploaded files from Goldman and that he selected a code repository website — the SVN Server — because it was not blocked by Goldman's security protocols. (Tr. 1125-27). He acknowledged encrypting the files and deleting the encryption software and bash history, as well as copying the files to his home computer, laptop, and thumb drive. (Tr. 1131-32). Aleynikov admitted that he erased his bash history because he was concerned about violating Goldman's security policies. (Tr. 1129). Aleynikov initially claimed, however, that he only intended to take open source — *i.e.*, publicly available

computer code not owned by Goldman — but, after the FBI informed Aleynikov that it would be reviewing the electronic evidence in this case, he then claimed that he had taken more files than he intended. (Tr. 1128-29). Aleynikov claimed to have taken files from Goldman because he wanted to review the open source code contained therein "like a person would in college, to go back and read a paper." (*Id.*).

B. The Defendant's Case

At trial, the defendant did not dispute that he uploaded code from Goldman without authorization. (Tr. 53-54, 57-58, 1556-57; *see also* Br. 7-8). Instead, Aleynikov argued that he lacked the requisite intent because, among other reasons, he intended to use only the open source, or free, software contained within the stolen code. (*Id.*). The defendant called one witness, Benjamin Goldberg, a professor of computer science. Professor Goldberg testified that he identified some open source computer code within the files taken from Goldman, but admitted that it was not his opinion that all of Goldman's high frequency trading system was "open source." (Tr. 1361). In fact "substantially more" of the Goldman files on the defendant's thumb drive contained Goldman copyright notices rather than open source notices. (Tr. 1361, 1366, 1426-29). And, Professor Goldberg testified that the "vast majority" of the files compressed within one of the tarball files bore Goldman copyright notices. (Tr. 1367). Although Aleynikov asserted that there was open source code embedded in files that purported to be proprietary to Goldman, Professor Goldberg identified only one such file out of the thousands taken by Aleynikov. (Tr. 1428-29).

C. The Sentencing

Following Aleynikov's conviction, the Probation Office prepared the Presentence Report in anticipation of sentencing. The Probation Office determined that Aleynikov's total offense level was 28 (PSR ¶ 41), that his Criminal History Category was I (PSR ¶ 44), and that the applicable Guidelines range was 78 to 97 months' imprisonment. (PSR ¶ 84). In calculating Aleynikov's offense level, the Probation Office calculated the loss amount to be just over $7 million. (PSR ¶¶ 24-26).

The Probation Office recommended a two-level upward adjustment for Aleynikov's abuse of a position of trust (PSR ¶ 35), but not a two-level enhancement for use of sophisticated means. (PSR at 22). The Probation Office recommended that Aleynikov receive a non-Guidelines sentence of 24 months' imprisonment. (PSR at 24).

Aleynikov primarily disputed the loss amount calculation and argued for a non-Guidelines sentence based, in part, on that imposed in *United States* v. *Samarth Agrawal*, 10 Cr. 417 (JSR), a case in which the defendant stole HFT code from a different bank. In *Agrawal*, the Honorable Jed S. Rakoff, United States District Judge for the Southern District of New York, sentenced the defendant to 36 months' imprisonment, below the applicable Guidelines range of 63 to 78 months' imprisonment. (A. 583, 589).

On March 18, 2011, Judge Cote conducted a sentencing proceeding in accordance with Federal Rule of Criminal Procedure 32. Judge Cote found that "the 7 to $20 million loss figure is amply supported by the evidence received at trial and corroborated by alternative calcula-

tions." (A. 559). The District Court also found that the Probation Office erred in not applying an enhancement for use of sophisticated means, a decision Aleynikov does not contest on appeal. (A. 561-62). Accordingly, the District Court found the Guidelines range to be 97 to 121 months' imprisonment.

After considering in detail and distinguishing the *Agrawal* case, Judge Cote sentenced Aleynikov to a term of 97 months' imprisonment, a term of three years' supervised release, and a fine of $12,500.

ARGUMENT

POINT I

The District Court Properly Denied Aleynikov's Motion to Dismiss Counts One and Two of the Indictment

The District Court throughly considered and properly rejected Aleynikov's arguments that the Indictment did not state a claim under the Economic Espionage Act of 1996 ("EEA") or the National Stolen Property Act ("NSPA"). Applying the "plain meaning" of the relevant terms of the EEA, the District Court held in its September 3, 2010 Opinion and Order that Goldman's HFT system, which trades in markets throughout the United States and around the world, was clearly "produced for" interstate and foreign commerce. (SPA 8-28). Likewise, Judge Cote found no tangibility requirement for prosecutions brought under Title 18, United States Code, Section 2314, and thus rejected Aleynikov's argument that the NSPA does not apply to intangible intellectual property such as the trading

system's source code. (SPA 32-39). The District Court's decision should be affirmed.

A. Applicable Law

An indictment may be challenged where it does not allege a crime within the terms of the statute. *United States* v. *Pirro*, 212 F.3d 86, 91-92 (2d Cir. 2000).

In this case, Aleynikov's challenge to the adequacy of the Indictment turns on the interpretation of statutory language. Generally, statutory construction "must begin with the language employed by Congress and the assumption that the ordinary meaning of that language accurately expresses the legislative purpose." *United States* v. *Albertini*, 472 U.S. 675, 680 (1985). Where "the statute's language is plain, 'the sole function of the courts is to enforce it according to its terms.'" *United States* v. *Ron Pair Enterprises, Inc.*, 489 U.S. 235, 241 (1989) (quoting *Caminetti* v. *United States*, 242 U.S. 470, 485 (1917)). When the statutory language is clear, there is no need to examine the statutory purpose, legislative history, or the rule of lenity. *See Boyle* v. *United States*, 129 S. Ct. 2237, 2247 (2009).

On appeal, "[t]he sufficiency of the indictment is a matter of law that is reviewed *de novo*." *See Pirro*, 212 F.3d at 92.

B. Discussion

1. Count One — Theft of Trade Secrets

Count One of the Indictment charges Aleynikov with theft of trade secrets under the EEA, in violation of Title 18, United States Code, Section 1832. That section provides:

> Whoever, with intent to convert a *trade secret, that is related to or included in a product that is produced for or placed in interstate or foreign commerce*, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly . . . without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information [is guilty of theft of trade secrets].

18 U.S.C. § 1832(a)(2) (emphasis added). The EEA does not define "product" or "produced for or placed in interstate or foreign commerce."

Aleynikov contends that Goldman's HFT system — which contains the trade secrets at issue — is not "produced for" commerce within the meaning of the EEA.[*]

---

[*] Aleynikov appears to have abandoned his contention below that the trading system was not a

Under Aleynikov's view, Section 1832 can apply only to trade secrets that are, or are intended to be, embodied in consumer products that are themselves shipped in interstate commerce. (Br. 24-30).

Aleynikov's arguments fail. The trading system, which uses sophisticated computer software to trade hundreds of millions of dollars of securities each year in markets around the world, was produced for interstate and foreign commerce. The trading system was created to trade securities and commodities in markets in the United States, Europe, and Asia (Tr. 332-40, 444-51); Goldman initially purchased the system for $500 million (Tr. 339); Goldman pays its programmers millions of dollars to develop and maintain the source code to the system (Tr. 449-50); and the system generates hundreds of millions of dollars in revenue for Goldman (Tr. 983). In addition, the source code itself traveled in interstate and foreign commerce: the source code was edited by Goldman programmers, such Aleynikov, at Goldman's offices in New York; was stored on a Goldman computer server in New Jersey; and was used by Goldman computers that were physically located

---

"product" within the meaning of Section 1832 in favor of arguing that the trading system was not "produced for" interstate commerce. In any event, applying the plain, ordinary meaning of the term "product," *i.e.*, "[t]hat which is produced by any action, operation, or work; a production; the result," 12 Oxford English Dictionary 565 (2d ed. 1989), Judge Cote properly found that there was "no doubt" that the trading system was a "product" within the meaning of the statute. (SPA 11-12).

around the world to trade on various markets. (Tr. 214-15, 444, 448). Further, as detailed below, the source code is inherently valuable because a market exists for it.

Thus, the trading system is "produced for" interstate or foreign commerce under any common-sense and ordinary reading of those terms. Indeed, the District Court found that "the sole purpose for which Goldman purchased, developed, and modified the computer programs that comprise the system was to engage in interstate and foreign commerce." (SPA 13).

The trading system is also "placed in" interstate and foreign commerce within the meaning of the EEA, using the common meaning of those terms.* As is clear from evidence discussed above, the trading system clearly maintains both a physical presence and an electronic presence in the stream of commerce as it executes scores of orders to trade securities and commodities around the world. Thus, the trading system has a very real presence in the stream of commerce and thus has been "placed in" commerce by Goldman.

---

* Because the District Court held that the system satisfied the "produced for" prong of the EEA, it never reached the Government's argument below that the system is also "placed in" commerce. This Court may nonetheless affirm the District Court's judgment on this ground. *See United States* v. *White*, 980 F.2d 836, 842 (2d Cir. 1992) (this Court "may affirm on any basis for which there is a record sufficient to permit conclusions of law, including grounds upon which the district court did not rely.").

The Government is not aware of any cases expressly addressing the issue raised by Aleynikov, and indeed, Aleynikov cites none in his Brief.[*] However, the legislative history of the EEA unambiguously supports a broad, and not a narrow, reading of Section 1832's terms. In enacting the EEA, Congress sought to "provide a comprehensive tool for law enforcement personnel to use to fight theft of trade secrets." *United States* v. *Yang*, 281 F.3d 534, 543 (6th Cir. 2002). Congress recognized both the importance of intellectual property to the nation's economy and the threat posed by the theft of such information. *See*, *e.g.*, H.R. Rep. No. 104-788, at 4, 6, *reprinted in* 1996 U.S.C.C.A.N. 4021, 4023-24 (1996) (recognizing the growing importance of "proprietary economic information" and finding that "[a]s the nation moves into the high-technology, information age, the value of these intangible assets will only continue to grow"); *see also* Opening Statement of Sen. Arlen Specter in S. Hrg. 104-499, 1996 WL 90824, at 2 (1996) ("The development and production of proprietary economic information is an integral part of U.S. business and is thus essential to preserving the competitiveness of the U.S. economy."). Indeed, one of Congress' primary concerns was preventing employees,

---

[*] In addition to the *Agrawal* case, which also involves the theft of HFT code, the Government is aware of at least one other case brought under Section 1832 that involved trade secrets not embodied in a consumer product that itself moves in commerce. *See United States* v. *Nosal*, No. 08 Cr. 237 (MHP), 2009 WL 981336 (N.D. Cal. Apr. 13, 2009) (information from an executive search firm's database).

such as Aleynikov, from stealing their employer's trade secrets — exactly the situation at issue in the instant case. *See* H.R. Rep. No. 104-788, at 7, 1996 U.S.C.C.A.N. at 4026.[*]

Congress found that there was no comprehensive criminal law that protected proprietary information in a thorough and systematic manner. *See* S. Rep. 104-359, at 9; H.R. Rep. No. 104-788, at 6-7, *reprinted in* 1996 U.S.C.C.A.N. at 4024-25. Accordingly, Congress promulgated the EEA to "extend vital federal protection to another form of proprietary economic information — trade secrets." H.R. Rep. No. 104-788, at 4, *reprinted in* 1996 U.S.C.C.A.N. at 4023. In signing the EEA into law, President Clinton stated that the statute was designed to "protect the trade secrets of *all businesses operating in the United States*, foreign and domestic alike, from economic espionage and trade secret theft." Statement by President William J. Clinton upon Signing H.R. 3723, 32 Weekly Comp. Pres. Doc. 2040 (Oct. 14, 1996), *reprinted in* 1996 U.S.C.C.A.N. 4034, 4034 (emphasis added). After reviewing this history, the District Court correctly found that it

---

[*] The examples found in the legislative history do not compel Aleynikov's cramped reading of the statute. (Br. 28). Indeed, as correctly noted by the District Court (*see* SPA 17-18 n.7), one of the examples in the legislative history is similar to the facts of the instant case. *See* S. Rep. No. 104-359, at 9 (employee theft of source code from a firm that supplied "software technology to various government projects, primarily in NASA astrophysics activities").

fully supported its interpretation of the statute. (SPA 13-17).*

Aleynikov contends, however, that because the trading system was proprietary and not intended for sale or to produce goods for sale, its theft cannot violate Section 1832. For support, Aleynikov relies on interpretations of the Fair Labor Standards Act, 29 U.S.C. § 201 *et seq.* (the "FLSA"), which addresses labor standards in "industries engaged in . . . the production of goods for commerce." 29 U.S.C. § 202(a). Aleynikov's reliance on the FLSA is misplaced. The District Court correctly found that, unlike the FLSA, Section 1832 does not refer to the "production of *goods* for commerce," but "rather more generally to any '*product* produced for' commerce." (SPA 22). Aleynikov provides no explanation for why the definition of the terms of the FLSA, which deals with labor standards, should control the interpretation of Section 1832, which deals with intellectual property.

But perhaps more importantly, the FLSA itself does not support Aleynikov's position. The Supreme Court has expressly rejected Aleynikov's limited interpretation of the FLSA's "for commerce" requirement as meaning only the "production of goods *for transportation* in commerce." *See Alstate Const. Co.* v. *Durkin*, 345 U.S. 13, 15 (1953)

---

* Aleynikov asserts that omission of the "produced for" language from Section 1831, which deals with trade secret theft by foreign governments, means that Congress intended that Section 1832 cover a more limited set of trade secrets. Judge Cote correctly rejected this argument as having no basis in the legislative history. (SPA 15-18).

("We could not hold . . . that the only way to produce goods 'for commerce' is to produce them for transportation across state lines."); *see also Mitchell* v. *Owen*, 292 F.2d 71, 75 (6th Cir. 1961) ("That the production and use of the materials both occur in the same state is of no legal consequence, if the materials were produced for use in work upon instrumentalities of commerce.").[*] Further, the FLSA provides broad definitions for the terms "commerce," "goods," and "produced" that would cover the trading system. *See* 29 U.S.C. § 203(b) (defining "commerce" as "trade, commerce, transportation, *transmission*, or *communication*, among the several States or between any State and any place outside thereof" (emphasis added)); *id.* § 203(i) (defining "goods" as including, among other things, *"articles or subjects of commerce of any character*, or any part of ingredient thereof" (emphasis added)); *id.* § 203(j) (defining "produced" as "produced, manufactured, mined, handled, or *in any other manner worked on* in any State" (emphasis added)).[**]

---

[*] Thus, Aleynikov is incorrect in asserting that no precedent exists for Judge Cote's decision. For example, *Alstate*, which is cited in Aleynikov's brief, holds that goods are produced "for commerce" even if they are made and used entirely within a state so long as they are used *in connection* with interstate commerce. *See Alstate*, 345 U.S. at 15.

[**] Indeed, as the District Court noted in its opinion (SPA 23 n.12), this Court has held that the FLSA's jurisdictional element encompasses businesses engaged in intangible activities. *See Darr* v. *Mutual Life Ins. Co. of N.Y.*, 169 F.2d 262, 264 (2d Cir. 1948) (insurance

The FLSA regulation on which Aleynikov relies — 29 C.F.R. § 776.21(a) — also does not support his argument. (Br. 25-26). That regulation broadly defines "for commerce," to include among other things, "*transmission*[] or *communication* among the several States." 29 C.F.R § 776.21(a) (emphasis added). That regulation further provides that "particular goods are produced 'for' commerce when they are *produced with a view to their use, whether within or without the State*, in the direct furtherance of the movement of interstate or foreign commerce." *Id*. § 776.21(b)(2) (emphasis added). Accordingly, to the extent the FLSA is an appropriate analogue for interpreting the EEA, it is clear that cases and regulations under the FLSA support the application of the EEA to Aleynikov's theft.

Aleynikov also argues that products liability law supports his claim that the EEA should not be read to reach intangible proprietary items such as the trading system. (Br. 27-28). But products liability, almost by definition, is the wrong place to look for guidance in interpreting the EEA. Unlike the law of trade secrets, products liability law is concerned with physical harms caused by *tangible* consumer goods. *See*, *e.g.*, Restatement (Third) of Torts: Products Liability § 1 ("One engaged in the business of selling or otherwise distributing products who *sells or distributes a defective product is subject to liability for harm to persons or property caused by the*

---

policies); *Bozant v. Bank of N.Y.*, 156 F.2d 787, 790 (2d Cir. 1946) ("bonds, shares of stock, commercial paper, bills of lading and the like").

defect.") (emphasis added). Indeed, in *Gorran* v. *Atkins Nutritionals, Inc.*, 464 F. Supp. 2d 315, 324 (S.D.N.Y. 2006), the single case cited by Aleynikov on this point, the district court noted that "[p]roducts liability law focuses on the *tangible* world." 464 F. Supp. 2d at 324 (emphasis added). By contrast, the law of intellectual property is focused on confidential business information that may or may not be tangible but is valuable. As Congress recognized, such information may be "the keystone" to a company's "economic competitiveness," such that companies "spend many millions of dollars developing the information, take great pains and invest enormous resources to keep it secret, and expect to reap rewards from their investment." H.R. Rep. No. 104-788, at 4, *reprinted in* 1996 U.S.C.C.A.N. at 4023. For these reasons, Judge Cote correctly found that it would "be inappropriate to use a specialized definition of 'product' drawn from products liability law for a statute whose purpose is to broadly protect intellectual property."* (SPA 18-19; *see also id*. 11-12 & n.2).

Aleynikov relies on interpretations of Section 1832 found in the United States Attorney's Manual ("USAM")

---

* The definition of "product" in Black's Law Dictionary appears to be derived from the law of products liability and thus provides a specialized definition, not the word's plain, ordinary meaning. Instead, the ordinary meaning of "product" is more akin to "something produced by physical labor or intellectual effort: the result of work or thought." Webster's Third New International Dictionary 1810 (1993).

and the Department of Justice's Intellectual Property Crimes Manual ("IP Manual"). (Br. 29-30). These manuals, which are not binding and which disclaim any precedential effect,* do not address the specific facts of this case. Instead, for example, they provide guidance in cases where the product at issue is still under development and has not yet been sold in interstate commerce. *See* USAM 9-50.100; IP Manual 160-61. They also advise that the EEA does not apply to "pure services" including "technical skills" and "know-how" that are unrelated to any product — which is clearly not the situation here. IP Manual at 161. What is clear from the manuals is that, to the extent they even support the defendant's position,**

---

* The USAM states, in pertinent part:

> The Manual provides only internal Department of Justice guidance. It is not intended to, does not, and may not be relied upon to create any rights, substantive or procedural, enforceable at law by any party in any matter civil or criminal.

USAM 1-1.100, 1997 WL 1943989. Likewise, the IP Manual states, in pertinent part:

> This Manual is intended as assistance, not authority. The . . . conclusions herein . . . do not represent the official position of the Department of Justice or any other agency.

IP Manual at xvii-xviii; *see also* SPA 24.

** For example, the IP Manual emphasizes that "[t]he nexus to interstate or foreign commerce [in Section 1832]

their guidance is directed at the generic trade secrets theft, but not Aleynikov's sophisticated one.

Aleynikov further contends that "the district court's broad interpretation of the EEA's commerce element would destroy the balance between state and federal criminal prosecutions of trade secrets by making virtually every theft of a trade secret a federal crime." (Br. 40-41).

In this case, however, the Government's proposed reading of the EEA is not so broad as to convert a whole category of conduct traditionally proscribed only by the states into a federal offense. Indeed, to hold that the trading system was "produced for" and "placed in" interstate and foreign commerce simply cannot and does not convert every theft of a trade secret into a federal crime. As the District Court correctly noted, the trading system has a "strong and substantial connection to interstate and foreign commerce."[*] (SPA 25).

---

appears to have been intended *merely* to allow federal jurisdiction." IP Manual at 160 (emphasis added).

[*] Aleynikov takes this latter comment by the District Court and argues that the District Court "engrafted a requirement of a 'strong and substantial connection' to interstate commerce" on the statute. (Br. 33). The District Court, however, did no such thing. Judge Cote was merely distinguishing the trading system from matters at issue in other cases. (SPA 25-26 (analyzing *Jones* v. *United States*, 529 U.S. 848, 857 (2000); *United States* v. *Mennuti*, 639 F.2d 107, 113 (2d Cir. 1981); and *United States* v. *Perrotta*, 313 F.3d 33, 37 (2d Cir. 2002)). Judge Cote had already held that the trading system was "produced for"

In any event, as the District Court correctly noted (SPA 26-27), and as Aleynikov himself acknowledges (Br. 41), Congress has, in fact, chosen to alter the balance of state and federal prosecution of trade secret theft. The EEA's legislative history contains express findings by Congress that the available state laws "protect[] proprietary economic information only haphazardly," and that "[o]nly by adopting a *national scheme* to protect U.S. proprietary economic information can we hope to maintain our industrial and economic edge and thus safeguard our national security." S. Rep. 104-359, 11-12, 1996 WL 497065 (1996) (emphasis added); *see also* H.R. Rep. No. 104-788, *reprinted in* 1996 U.S.C.C.A.N. 4021, 4025 (1996) (finding that a "comprehensive federal criminal statute" "will serve as a powerful deterrent to this type of crime" and would "better facilitate the investigation and prosecution of [trade secret theft]"). Indeed, the Senate Report to the EEA states, "a Federal criminal law is needed because of the international and interstate nature of this activity, because of the sophisticated techniques used to steal proprietary economic information, and because of the national implications of the theft." S. Rep. No. 104-359, at 12. The Senate Report to the EEA also found that "[o]nly a few States have *any* form of criminal law dealing with the theft of this type of information. Most such laws are only misdemeanors, and they are rarely used by State prosecutors." S. Rep. No. 104-359, at 11 (emphasis added). Even today, by Aleynikov's count (Br. 40 n.5),

---

commerce under the "plain, ordinary meaning" of those terms. (SPA 13).

sixteen states still have no law expressly criminalizing the theft of trade secrets.

Accordingly, both the statutory language and legislative history show that the EEA was intended to reach Aleynikov's theft, and the District Court's decision should be affirmed.

2. Count Two — Interstate Transportation of Stolen Property

The stolen source code also falls squarely within the NSPA, which provides:

> Whoever *transports, transmits, or transfers* in interstate or foreign commerce any *goods, wares, merchandise, securities or money*, of the value of $5,000 or more, knowing the same to have been stolen, converted or taken by fraud [commits a crime].

18 U.S.C. § 2314 (emphasis added). Section 2314 does not define the terms "goods," "wares," or "merchandise." As the District Court correctly noted (SPA 30), this Court, following the Third Circuit, has interpreted these terms broadly to signify "'a general and comprehensive designation of such personal property or chattels as are *ordinarily a subject of commerce*.'" *In re Vericker*, 446 F.2d 244, 248 (2d Cir. 1971) (Friendly, J.) (quoting *United States* v. *Seagraves*, 265 F.2d 876 (3d Cir. 1959) (emphasis added). In *Vericker*, this Court held that "under some circumstances, *mere papers* may constitute 'goods,' 'wares,' or 'merchandise'" as long as they are "ordinarily bought and sold in commerce." *Id*. at 248 (citation omitted) (emphasis added). In *United States* v. *Bottone*, 365 F.2d 389 (2d Cir.

1966) (Friendly, J.), this Court held that copies and notes of stolen papers reflecting "manufacturing procedures" for a pharmaceutical company were "goods" within the meaning of Section 2314 because there was an illicit market for them. *Bottone*, 365 F.2d at 393.

Moreover, district courts in this and other Circuits have held that Section 2314 applies to confidential business information for which a market exists. *See United States* v. *Farraj*, 142 F. Supp. 2d 484, 487-88 (S.D.N.Y. 2001) (Marrero, J.) (attorney trial plan); *United States* v. *Caparros*, No. 85 Cr. 990 (JFK), 1987 WL 8653, at *3-4 (S.D.N.Y. Mar. 25, 1987) (secret business plans); *United States* v. *Alavi*, No. 07 Cr. 429 (PHX), 2008 WL 1971391, at *2 (D. Ariz. May 2, 2008) (stolen software); *United States* v. *Riggs*, 739 F. Supp. 414, 420 (E.D. Ill. 1990) (confidential information related to emergency 911 services), *sentence aff'd*, 967 F.2d 561 (11th Cir. 1992). *But see United States* v. *Kwan*, No. 02 Cr. 241 (DAB), 2003 WL 22973515, at *6 (S.D.N.Y. Dec. 17, 2003) (travel agency's proprietary contact lists and rate sheets were not "goods, wares, or merchandise" because no evidence of a market for such information exists).

Aleynikov contends, however, that because the source code is intangible, it cannot be "a good, ware or merchandise" under the statute. (Br. 19). The District Court properly found that "Aleynikov's attempt to graft a tangibility requirement onto § 2314 is unavailing." (SPA 32). The District Court correctly held that the "text of § 2314 makes no distinction between electronic and other modes of transfer across state and international lines," and that, "[t]o the contrary, anyone who 'transmits' or 'trans-

fers' stolen property, even if the mode of such transmission or transfer is not physical, violates § 2314." (SPA 33).

Indeed, in *United States* v. *Gilboe*, 684 F.2d 235 (2d Cir. 1982), this Court held that the electronic transfer of funds was covered by the NSPA, noting that "[t]he primary element of this offense, *transportation*, does not require proof *that any specific means of transporting were used*." *Id.* at 238 (citation omitted) (emphasis added).* And, in *Bottone*, this Court observed that "when the physical form of the stolen goods is secondary in every respect to the matter recorded in them, the transformation of the information in the stolen papers into a tangible object never possessed by the original owner should be deemed immaterial." *Bottone*, 365 F.2d at 393-94.

Aleynikov relies on Judge Friendly's observation in *Bottone* that "where no *tangible objects* were ever taken or

---

* Congress later amended Section 2314 to confirm that it applies to electronic transfers. *See United States* v. *Piervinanzi*, 23 F.3d 670, 678 n.6 (2d Cir. 1994). Aleynikov argued below that this amendment was limited to wire transfers of money, an argument he has not renewed on appeal. In any event, as Judge Cote noted, nothing in the text of the statute requires that the term "transmits" be limited to wire transfers of money. (SPA 33 n.19). Indeed, the legislative history of the amendment reveals that "the amendment to § 2314 was designed to codify appellate court holdings that 18 U.S.C. [§] 2314 is not limited to the *physical* transportation of stolen or fraudulently acquired *money or property*." *Piervinanzi*, 23 F.3d at 678 n.6 (citation omitted) (emphasis added).

transported, a court would be hard pressed to conclude that 'goods' had been stolen and transported within the meaning of § 2314." *Bottone*, 365 F.2d at 393 (emphasis added). Aleynikov ignores, however, the second half of Judge Friendly's observation, which clarifies the situation this Court envisioned: "[T]he statute would presumably not extend to the case where a carefully guarded secret formula was *memorized, carried away in the recesses of a thievish mind and placed in writing only after a boundary had been crossed*." *Id.* (emphasis added). Unlike the hypothetical case in which a defendant *memorizes* a trade secret, Aleynikov was charged and convicted of electronically transmitting the stolen source code across state and international lines and then physically transporting it with him to Chicago on a flash drive and laptop.

Aleynikov is not correct in asserting that "[e]very court of appeals to consider the question has held that § 2314 does not apply to intellectual property, such as the source code here." This Court and at least two other courts of appeal have held that Section 2314 applies to trade secrets — in other words, intellectual property — for which a market exists. *See Bottone*, 365 F.2d at 391 (holding that Section 2314 applies to a pharmaceutical company's "secret processes" and "instructions for . . . drugs' manufacture"); *United States* v. *Greenwald*, 479 F.2d 320, 321 (6th Cir. 1973) (applying Section 2314 to secret chemical formulas); *United States* v. *Seagraves*, 265 F.2d at 878 (holding that Section 2314 applies to an oil company's confidential geophysical and geological maps); *Cf. United States* v. *Martin*, 228 F.3d 1, 13-15 (1st Cir. 2000) (upholding conviction of conspiracy to transport in interstate

commerce various stolen trade secrets, including a company's proprietary computer software).*

To be sure, the Tenth Circuit's decision *United States* v. *Brown*, 925 F.2d 1301 (10th Cir. 1991), held that a "'computer program itself is an intangible intellectual property, and as such, it alone cannot constitute goods . . . within the meaning of [§] 2314.'" *Id.* at 1307-08. As the District Court held (SPA 38), however, *Brown* is neither binding nor persuasive because it misreads the Supreme Court's decision in *Dowling* v. *United States*, 473 U.S. 207 (1985). *Dowling*'s interpretation of Section 2314 in the context of copyright infringement was focused not on creating a tangibility requirement to the NSPA, but rather was focused on the "physical identity between the items unlawfully obtained and those eventually transported." *Dowling*, 473 U.S. at 216. *Dowling* involved bootleg recordings of Elvis Presley singing copyrighted songs. *Id.* at 210-11. In *Dowling*, the Government did not allege that the defendant "wrongfully came by the phonorecords actually shipped" or that the bootlegged phonorecords "were 'the same' as the copyrights in the musical compositions that he infringed'" and accordingly, the Supreme Court found no violation of Section 2314. *Dowling*, 473 U.S. at 214. By contrast, in this case, "the item that Aleynikov physically stole is identical to the item that

---

* To the extent, however, that the court of appeals in *Martin* followed the Tenth Circuit's decision in *United States* v. *Brown*, 925 F.2d 1301 (10th Cir. 1991), the Government submits that it was incorrectly decided, for the reasons discussed below.

Aleynikov allegedly transmitted and transported in interstate and foreign commerce: the source code in its electronic format." (SPA 38). Thus, this case passes *Dowling*'s identity test.*

---

* Further, the Court's decision in *Dowling* appears to be motivated in part by the special circumstances presented by copyright law itself, none of which are applicable in the trade secret context. The *Dowling* Court stated that "Congress had no intention to reach copyright infringement when it enacted § 2314." *Dowling*, 473 U.S. at 226. The Court reached this conclusion after carefully analyzing the Constitutional and statutory bases for copyright law, the particular rights afforded to copyright holders, and the types of copyright infringement that Congress has determined merit criminal sanction. *Id*. at 216-226. The Supreme Court stated that copyright is "no ordinary chattel," because it "comprises a series of carefully defined and carefully delimited interests to which the law affords corresponding exact protections," and therefore "does not easily equate with theft, conversion, or fraud." *Id*. at 216-17. And while the Supreme Court in *Dowling* makes reference to "kindred fields of intellectual property law," such as patents and trademarks, *see Dowling*, 473 U.S. at 226, it does not make any reference to trade secrets or confidential business information. The Court's reasons for excluding copyrighted works from the scope of Section 2314 do not apply to trade secrets. For example, whereas the Supreme Court notes that misappropriation of copyrighted materials is not even called "theft" under copyright law, *see id*. at 217, the misappropriation of trade secrets is called "theft" under

Returning to *Brown*, Judge Cote correctly found that the Tenth Circuit "place[d] undue emphasis on *Dowling*'s use of the term 'physical,' which . . . was not critical to the Court's decision." (SPA 38). The District Court further observed that *Brown* fails to acknowledge that "after *Dowling*, Congress amended § 2314 to add the term 'transmits' to cover transfers of non-physical forms of stolen property." (SPA 38).*

Aleynikov also relies on *United States* v. *Stafford*, 136 F.3d 1109 (7th Cir. 1998). *Stafford*, however, is distinguishable on its facts and not sufficiently detailed to provide guidance. The issue in *Stafford* was whether "Comdata codes," which were transmitted to truck drivers to allow the drivers to obtain cash at truck stops, were "goods, wares, [or] merchandise" under Section 2314. *Stafford*, 136 F.3d at 1111. The Seventh Circuit held that

---

trade secrets law. And whereas copyright holders are compelled by law to license their works to others under certain conditions, and are compelled to allow others the "fair use" of their copyrighted material, *see id*., no such conditions are imposed on the holders of trade secrets. Accordingly, there is no reason to believe that the Supreme Court intended to place trade secrets out of the reach of Section 2314.

* At least two other district courts have found *Brown* similarly unpersuasive. *See United States* v. *Farraj*, 142 F. Supp. 2d at 489 ("*Brown* does not square with" *Bottone*, and "may be based on a misapplication of *Dowling*.") (Marrero, J.); *United States* v. *Alavi*, 2008 WL 1971391, at *2.

these codes were "simply sequences of digits," which "have no value in themselves" but are merely "information," and therefore not "goods, wares or merchandise." *Id.* at 1114-15. By contrast, the source code in this case "is of obvious commercial value, whether in hard copy or electronic format." (SPA 36 n.21).

Aleynikov cites to cases and legislative history explaining Congress's concerns about the limitations placed on the scope of Section 2314 by *Dowling* and *Brown* and how those concerns prompted, in part, the passage of the EEA. (Br. 18-20). Congress's concerns merely reflect the uncertainty created by *Dowling* and *Brown*, but are not a persuasive reason to find that Goldman's proprietary source code is not a "good" within the meaning of Section 2314. In any event, the EEA and NSPA are different criminal statutes that "target completely different evils." (SPA 39).

Finally, Aleynikov contends that the NSPA is "a Prohibition-era statute that did not foresee — or attempt to prohibit — the transmission of intangible property." (Br. 19). There is nothing, however, in the text of Section 2314 itself that expressly limits the application of the statute to the physical transportation of tangible property. On the contrary, the term "transmits" in Section 2314 expressly *includes* the electronic *transmission* of stolen money or property. *See Piervinanzi*, 23 F.3d at 678 n.6 (amendment "designed to codify appellate court holdings that 18 U.S.C. [§] 2314 is not limited to the physical transportation of stolen or fraudulently acquired money or property.").

In sum, it is clear that, under Section 2314, confidential business information, such as trade secrets, are "goods" regardless of whether they are transmitted and transported in tangible or intangible form.* Accordingly, the District Court properly denied Aleynikov's motion to dismiss Count Two.

POINT II

The Evidence Was Sufficient

The District Court properly rejected Aleynikov's sufficiency challenges because the evidence established (i) Aleynikov's intent to injure Goldman, as required by the EEA and (ii) that the stolen source code was a "good," "ware," or "merchandise" under Section 2314. (SPA 64-75).**

---

* Indeed, the record reflects that it would have been far more difficult for Aleynikov to transport the 500,000 lines of stolen code, and it would have been far less "commercially valuable," in paper format. (SPA 34).

** Aleynikov has abandoned his contentions below that the evidence was also insufficient to show that (i) he intended to steal Goldman's proprietary source code rather than merely take open source code allegedly embedded within Goldman's system and (ii) he took Goldman's code with the intent to benefit himself or Teza. Judge Cote rejected each of these contentions after carefully reviewing the evidence. (SPA 65-71).

A. Applicable Law

In evaluating a sufficiency challenge, this Court reviews the evidence "not in isolation but in conjunction," *United States* v. *Matthews*, 20 F.3d 538, 548 (2d Cir. 1994), and "in the light most favorable to the government," drawing all reasonable inferences in its favor, *United States* v. *Gaskin*, 364 F.3d 438, 459 (2d Cir. 2004). The Government "need not negate every theory of innocence." *United States* v. *Lee*, 549 F.3d 84, 92 (2d Cir. 2008). "[T]o avoid usurping the role" of the jury, *United States* v. *Autuori*, 212 F.3d 105, 114 (2d Cir. 2000), the Court must "resolve all issues of credibility in favor of the jury's verdict." *United States* v. *Desena*, 287 F.3d 170, 177 (2d Cir. 2002).

The "task of choosing among competing, permissible inferences is for the fact-finder, not for the reviewing court." *United States* v. *McDermott*, 245 F.3d 133, 137 (2d Cir. 2001). This approach "gives full play to the responsibility of the trier of fact fairly to resolve conflicts in the testimony, to weigh the evidence, and to draw reasonable inferences from basic facts to ultimate facts." *Jackson* v. *Virginia*, 443 U.S. 307, 319 (1979). Finally, a verdict may be based entirely on circumstantial evidence. *United States* v. *D'Amato*, 39 F.3d 1249, 1256 (2d Cir. 1994).

B. Discussion

1. Theft of Trade Secrets

The trial evidence was more than sufficient to show that in stealing the source code, Aleynikov intended to injure Goldman. The EEA requires proof that a defendant act with "intent to convert a trade secret . . . to the eco-

nomic benefit of anyone other than the owner thereof" and further that the defendant, "intend[] and know[] that the offense will injure any owner of that trade secret." 18 U.S.C. § 1832(a). With respect to the injury element, "[t]he legislative history indicates that this requires 'that the actor knew or was aware to a practical certainty that his conduct would cause such a result,'" *United States* v. *Hsu*, 155 F.3d 189, 196 (3d Cir. 1998) (quoting S. Rep. No. 104-359, at 15), but does not require proof of "malice or evil intent." H.R. Rep. No. 104–788, at 11-12 (1996), *reprinted in* 1996 U.S.C.C.A.N. 4021, 4030.

The jury's verdict on Count One is well-supported by the evidence. For example, it was undisputed that HFT is a highly secretive and highly competitive field in which firms protect the confidentiality of their systems for fear of losing any competitive advantage they may have over other firms. (Tr. 339-41, 346-48, 447-48, 679-711, 786-87). For example, Schlesinger testified that "if you share what you believe to be important aspects of your system with others, that would just help their profitability and hurt yours." (Tr. 447). Benjamin Van Vliet testified that no firm engaged in HFT discloses information about its system because that "would be perceived to be giving away a secret that could infringe on [the] ability to make money." (Tr. 695).

Malyshev further testified that high-frequency firms do not share proprietary information because it "may give competitors hints about what you do and how you do it." (Tr. 808). Finally, Demian Kosofsky testified that HFT firms do not publicly disclose their software because the software constitutes "one of their competitive advantages."

(Tr. 873). Accordingly, Judge Cote correctly found that the "extensive evidence" establishing "the secretive nature of the high frequency trading business" and the measures Goldman took to protect its code was sufficient for the jury to find that Aleynikov intended to harm Goldman and knew that his decision to steal Goldman's code and share it with a competitor would harm Goldman. (SPA 73).*

Furthermore, the evidence established various ways that Goldman could be harmed if a competitor were to

---

* Moreover, as Judge Cote correctly found, the jury could have concluded that the elaborate measures taken by Aleynikov to stealthily steal Goldman's code and thereafter delete the records of this theft demonstrated Aleynikov's consciousness that his actions would harm Goldman. (SPA 73). Aleynikov contends, however, that it would be "far more rational" for the District Court to have credited his post-arrest statement (in which he disclaimed any intent to harm his former employer) over the inference that Aleynikov's concealment efforts demonstrated that he intended to harm Goldman. (Br. 46). However, in weighing a sufficiency challenge, it is not appropriate for the District Court to choose among competing inferences offered by the parties. *See United States* v. *McDermott*, 245 F.3d at 137. In any event, Aleynikov's defense is not "far more rational," because, as Judge Cote correctly observed, it would have been easier for Aleynikov to find open source code online rather than "undertaking the difficult and painstaking task of separating any open source code embedded in the proprietary code." (SPA 69-70).

obtain its source code. For example, Paul Walker, a managing director at Goldman, testified:

> This is a very competitive market *where the nature of competition involves knowing the algorithm and having a capability.* So it's the practice inside the industry to develop your algorithm and develop your capability and then maintain it as a secret."
>
> [A competitor with Goldman's code] could have several forms of advantage. . . . *[T]hey could skip decades of work*. They could see what our intent and our algorithms were, and our business logic, *so they can understand how we would make prices or generate trades*. And they would have access to the infrastructure parts of our software, which have years of experience of making it work . . . .

(Tr. 346-48 (emphasis added)).

Similarly, Schlesinger testified that:

> It would . . . enable a competitor to compete with us, whether it's because they have improved speed because of some of our software, or if their time to market is reduced because they have software they can now deploy, *that would impact our P&L* [profit and loss].

(Tr. 479-80) (emphasis added)).* Aleynikov's argument that harm to Goldman is "speculative" "unless a thief generated the same prices and trades as Goldman" (Br. 44-45), is belied by this testimony, which the jury was entitled to credit.**

Aleynikov also claims that Goldman could not have been harmed because Teza was never going to compete directly against Goldman. For this, Aleynikov relies principally on Malyshev's testimony that Malyshev (i) did not consider Goldman to be a serious competitor in HFT, (ii) did not want Goldman's source code, and (iii) did not intend to trade options. (Br. 43).

As Judge Cote found, however, Aleynikov's reliance on Malyshev's testimony here is misplaced. (SPA 72). First, although Malyshev stated that, apart from options trading, he did not think Goldman was a "significant competitor" (Tr. 832-33), Malyshev also admitted to having no personal knowledge of Goldman's HFT business, the strategies it uses, or how much money it makes. (Tr. 863-64). Other evidence at trial showed that Goldman

---

* In addition, witnesses gave detailed testimony under seal of the many ways the specific trade secrets Aleynikov stole gave Goldman a competitive advantage. (Tr. 533-42; 720-27; 986-89; 1042-43).

** Judge Cote further correctly found that the jury was entitled to rely on evidence of Aleynikov's prior infringement of intellectual property to establish intent (SPA 69), which was properly admitted pursuant to Rule 404(b), a decision which Aleynikov does not contest on appeal. (Tr. 1145-47, 1178-80, 1314-24).

was one of the most highly-respected firms in the HFT business, that it generated hundreds of millions of dollars, and that it competed with Citadel, Malyshev's former employer. (Tr. 340, 670-71, 902-83). Second, the jury was entitled to discount Malyshev's claim that he would not use another firm's software (Tr. 833), because Teza had no system in place to prevent the use of another firm's source code, and in fact, Aleynikov successfully uploaded Goldman files to Teza's system undetected. (Tr. 865, 882-84; 1233-54). Furthermore, Teza needed to develop a vast array of software before it could start trading — more than would be feasible on the time frame established by Malyshev. Teza needed software that (i) listens to a price feed from the markets in which it would trade; (ii) places orders on those markets; (iii) builds order books; and (iv) monitors its system. (Tr. 874-75). Aleynikov stole components that do all of these things, including a "substantial part of the infrastructure and some of the algorithms and market data connectivity" of Goldman's system.[*] (Tr. 365-66, 480-96, 977).

Finally, although Malyshev said that he was not initially interested in trading options at Teza (Tr. 788), he also testified that Teza would broadly pursue "*any* trading strategies that would . . . be part of high frequency business" and that the scope of its trading and the markets in which it would trade would expand over time, and might include options. (Tr. 787-88 (emphasis added)). Given the

---

[*] Van Vliet testified that the stolen code would give a "tremendous competitive advantage" to a competitor, "particularly to a start-up." (Tr. 723).

time frame established for Teza, and the advantages presented by Aleynikov's stolen code, the jury was entitled to discount Malyshev's claimed interests and infer that Aleynikov would create a system for Teza that necessarily would exploit the same trading opportunities identified in the stolen code. (Tr. 981-82).*

2. Interstate Transportation of Stolen Property

The trial evidence was more than sufficient to permit an inference that there is a market for the source code Aleynikov stole. Section 2314 requires that the Government prove that the stolen items transported across state lines be "goods, wares, merchandise, securities or money" worth "$5,000 or more." 18 U.S.C. § 2314. This Court has held that "goods," "wares," and "merchandise" means "a general and comprehensive designation of such personal property or chattels as are ordinarily a subject of commerce." *In re Vericker*, 446 F.2d at 248 (citation omitted); *see also United States* v. *Bottone*, 365 F.2d 389, 391-92 (2d Cir. 1966) (finding stolen microorganisms and copies of papers containing secret processes to be covered by Section 2314 because of evidence that an illicit market existed for them).

As the District Court held, the evidence "established that Aleynikov took a very substantial portion of the

---

* In *Agrawal*, Judge Rakoff rejected a similar argument, made at sentencing, regarding Agrawal's intent to harm his former employer, as "totally contrary to common sense." (A. 576-79).

source code for the Goldman HFT system, including the entirety of several critical components of the system" that "would be highly valuable to a competitor." (SPA 74). The evidence also showed that "portions of the Goldman system were acquired when the firm purchased Hull Trading Company for the substantial sum of $500 million and that there were commercially available, expensive substitutes for several components of the Goldman trading system." (SPA 74; *see* Tr. 339-40, 483-91, 540-42, 982, 989). Finally, the Government's expert witness testified that he had been hired by trading firms to develop custom-made components for those company's HFT systems. (Tr. 709-11). Accordingly, the Government produced ample evidence for the jury to conclude that there was a market for the stolen computer code.

Aleynikov argues that the Government's evidence regarding a market for entire HFT systems "has *no tendency* to make the existence of a market for individual components more or less probable," and is therefore "irrelevant." (Br. 23-24 (emphasis added)). This argument defies common sense. A market for entire HFT systems makes it more likely that there will be markets for components of those systems, just as a market for finished automobiles makes it more likely that there will be markets for automobile parts. In any event, as described above, the Government's evidence also showed that there is a market for component parts of a high frequency trading system, such as those stolen by Aleynikov.[*]

---

[*] Aleynikov's reliance on *United States* v. *Greenwald*, 479 F.2d 320 (6th Cir. 1973), is misplaced.

POINT III

The District Court Properly Admitted Evidence of a Market for HFT Systems

As noted above, the market for entire HFT systems tends to show a market for parts of an HFT system, and therefore the District Court acted well within its discretion in admitting that evidence.

Trial courts enjoy broad discretion to decide evidentiary issues, *see*, *e.g.*, *United States* v. *Khalil*, 214 F.3d 111, 122 (2d Cir. 2000), and this Court reviews a district court's evidentiary rulings only for abuse of discretion. *See United States* v. *Taubman*, 297 F.3d 161, 164 (2d Cir. 2002). Federal Rule of Evidence 401 defines "relevant evidence" as "evidence having any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence." Fed. R. Evid. 401. "Particular deference is accorded to a ruling of the trial judge with respect to relevancy," because the trial judge

---

(Br. 22). In *Greenwald*, the Sixth Circuit merely noted that, in a case in which the defendant stole secret chemical formulas from his employer, the Government had adduced evidence of (i) market for the finished products manufactured with the stolen formulas and (ii) a market for the formulas themselves. *United States* v. *Greenwald*, 479 F.2d at 321. The Sixth Circuit was not called upon to decide whether evidence of a market for finished products, alone, was sufficient to support the defendant's conviction, and therefore rendered no opinion on that issue. *See id*.

"has a familiarity with the development of the evidence and the jury's reaction to it which an appellate court cannot equal." *United States* v. *Southland Corp.*, 760 F.2d 1366, 1375 (2d Cir. 1985) (Friendly, J.).*

Accordingly, there was no error in admitting the hull evidence. Moreover, in light of the evidence of a market for components, any error was harmless.

POINT IV

The Government's Proof at Trial Did Not Constructively Amend the Indictment

In addition to the source code, Aleynikov stole other materials from Goldman relating to its trading system. Admission of evidence regarding these materials was entirely proper and did not constructively amend the Indictment because there was no substantial likelihood that Aleynikov was convicted of an offense other than what was charged in the Indictment. (SPA 90-93). Nor was a limiting instruction necessary because the admission of the evidence was not unfairly prejudicial or constrained by Federal Rule of Evidence 404(b).

---

* As Judge Cote observed below, Aleynikov has failed to identify "any ground" under Federal Rule of Evidence 403 to justify exclusion of the evidence. (A. 58-59; SPA 74-75).

A. Applicable Law

1. Constructive Amendment

An indictment has been constructively amended when the evidence or the jury charge "so alters an essential element of the charge that, upon review, it is uncertain whether the defendant was convicted of conduct that was the subject of the grand jury's indictment." *United States* v. *Rigas*, 490 F.3d 208, 227 (2d Cir. 2007) (internal quotation marks omitted). This Court, however, has "consistently permitted significant flexibility in proof, provided that the defendant was given notice of the core of criminality to be proven at trial." *Rigas*, 490 F.3d at 228 (internal quotation marks and footnote omitted). "[P]roof at trial need not, indeed cannot, be a precise replica of the charges contained in an indictment." *United States* v. *Heimann*, 705 F.2d 662, 666 (2d Cir. 1983).

This Court reviews the District Court's conclusion that there was no constructive amendment *de novo*. *See United States* v. *McCourty*, 562 F.3d 458, 469 (2d Cir. 2009).

2. Background Evidence

Under Rule 404(b) of the Federal Rules of Evidence, evidence of prior acts is admissible to show "motive, opportunity, intent, preparation, plan, knowledge, identity, or absence of mistake or accident." Fed. R. Evid. 404(b). However, evidence of uncharged criminal activity is not considered "other crimes" evidence subject to Rule 404(b) "if it arose out of the same transaction or series of transactions as the charged offense, if it is inextricably intertwined with the evidence regarding the charged offense, or if it is necessary to complete the story of the crime on

trial." *United States* v. *Carboni*, 204 F.3d 39, 44 (2d Cir. 2000).

This Court reviews a district court's evidentiary rulings only for abuse of discretion. *See United States* v. *Taubman*, 297 F.3d 161, 164 (2d Cir. 2002). Moreover, an error in admitting evidence should be disregarded if the error is harmless. *See* Fed. R. Crim. P. 52(a) ("Any error . . . which does not affect substantial rights shall be disregarded."); *United States* v. *Wilson*, 605 F.3d 985, 407 (D.C. Cir. 2010) (finding that district court's refusal to strike evidence of defendant's prior bad acts or provide a limiting instruction to be harmless error). For an error to be deemed harmless, the court is "not required to conclude that it could not have had any effect whatever; the error is harmless if we can conclude that the testimony was unimportant in relation to everything else the jury considered on the issue in question, as revealed in the record." *United States* v. *Rea*, 958 F.2d 1206, 1220 (2d Cir. 1992) (internal quotation marks omitted).

B. Relevant Facts

In addition to the source code, Aleynikov encrypted and uploaded from Goldman's computer system to the SVN Server, and then downloaded to his home computer, the refm materials — confidential business information related to Goldman's HFT system including evaluations of commercially available HFT components; evaluations of hardware and computer operating systems; and diagrams of Goldman's computer networks and programs. (Tr. 498-509, 1098, 1208; GX 108A - GX 108L).

At the time these exhibits were received into evidence, Aleynikov conducted a *voir dire* but did not object or request a limiting instruction. (*Id*.).

The Government's HFT expert testified that these materials would be useful to a competitor because, among other things, they show Goldman's solutions to problems that firms engaged in HFT commonly face. (Tr. 713-18). Aleynikov again did not object to the refm materials during this testimony.

A few days later, Aleynikov submitted a written motion to strike the refm materials. (Tr. 771-79). Judge Cote denied the motion, holding that "[t]he indictment is very clear that the defendant is charged with [the theft] of Goldman's computer code," and indicated that the jury charge would clearly reflect this. (Tr. 778). Judge Cote found that "[w]hether the defendant took additional items proprietary to Goldman . . . during the same set of thefts alleged by the government, that are integral to the efficient use of the stolen code . . . is highly relevant and probative and properly admissible." (*Id*.). Further, the District Court held that the refm materials do not implicate Federal Rule of Evidence 404(b) because they are "part of the same underlying criminal conduct alleged here and properly before the jury for them to consider." (Tr. 778-79).

In its summation, the Government reviewed the testimony concerning the refm materials and argued to the jury that Aleynikov's downloading of the refm materials "shows what he intended to do with the *source code* that he also downloaded. He intended to *use the code* he downloaded for the benefit of himself and Teza to set up Teza's [HFT] system." (Tr. 1465-66 (emphasis added)).

In instructing the jury, the District Court stated that in order to convict on Count One, it must be proven that Aleynikov "uploaded, downloaded, copied or transmitted *computer source code* owned by Goldman Sacks for use in its [HFT] system." (Tr. 1543 (emphasis added)). Similarly, the District Court instructed the jury that to convict on Count Two, it must be convinced that Aleynikov "transported, transmitted, or transferred Goldman' *computer code* for use in its [HFT] system in foreign or interstate commerce." (Tr. 1548 (emphasis added)). The instructions and the Court's description of the Indictment thus related solely to the theft and interstate transportation of source code, not the refm materials. (Tr. 1543, 1548-49).

C. Discussion

Asserting that the Government "relied heavily" on the refm materials, Aleynikov argues that "[t]here is no way of knowing whether his conviction was . . . inappropriately based on the theft and transportation of the [refm materials]." (*Id.*)

The trial record reveals no basis for the jury to have been confused regarding the nature of the charges in this case. The Indictment itself, which was provided to the jury, charges Aleynikov with the theft and interstate transportation of source code and does not even mention the refm materials. (A. 20-33). Similarly, the District Court's jury charge only references source code as the material that was allegedly stolen and transported, and Aleynikov does not contend that there was anything about the jury charge itself that could have misled the jury. (Tr. 1543, 1548-49); *cf. United States* v. *Salameh*, 152 F.3d 88, 116 (2d Cir.1998) ("'[J]uries are presumed to

follow their instructions.'" (alteration in original) (quoting *Zafiro* v. *United States*, 506 U.S. 534, 540 (1993))). The Government was also clear in its summation that the refm materials were introduced to demonstrate Aleynikov's intent in stealing the source code. (Tr. 1465-66). Accordingly, there is nothing about the introduction of the refm materials that "so alters an essential element of the charge that, upon review, it is uncertain whether the defendant was convicted of conduct that was the subject of the grand jury's indictment." *Rigas*, 490 F.3d at 227.

Nor was there any abuse of discretion in the District Court's decision that no limiting instruction was required. Judge Cote held that the refm materials "shed further light on Aleynikov's intended use for the stolen source code, providing further corroboration that he took the code for the purpose of building Teza's high frequency trading platform." (SPA 93). According, Judge Cote found that the refm materials "was not constrained by Rule 404(b)" (*id.*), and therefore no limiting instruction was necessary.

Even if a limiting instruction was necessary, the District Court's failure to provide one was harmless error. The theft of the refm material was, if anything, less pernicious than the theft of the code itself. In addition, the trial focused overwhelmingly on Aleynikov's theft and transportation of Goldman's source code. Given the clarity of the Indictment, the jury charge, and the parties' summations, there is no chance that the jury was confused about the nature of the charges in this case, or about what they needed to find to convict.

POINT V

Aleynikov's Sentence Was Procedurally and Substantively Reasonable

Aleynikov challenges the sentence imposed by the District Court on two grounds: (i) that the sentence was procedurally unreasonable because the District Court improperly calculated the loss amount under the Guidelines as being more than $7 million, but not more than $20 million and because Aleynikov did not intend to harm Goldman, and (ii) that the sentence was substantively unreasonable because there was an unwarranted sentencing disparity between Aleynikov and the defendant in *Agrawal*.

These contentions are without merit. Aleynikov fails to show that the District Court clearly erred (or indeed, committed any error) in calculating the loss amount. Further, the District Court (and the jury, in returning a conviction under the EEA) properly rejected Aleynikov's contention that he did not intend to harm Goldman. With respect to the sentence in *Agrawal*, the District Court took great care to distinguish circumstances of *Agrawal* and to explore fully all the sentencing factors that supported the sentence imposed.

A. Applicable Law

This Court's review of a district court's sentence "encompasses two components: procedural review and substantive review." *United States* v. *Cavera*, 550 F.3d 180, 189 (2d Cir. 2008) (en banc). A district court commits procedural error where, among other things, it "makes a mistake in its Guidelines calculation." *Id*. at 190. In

considering challenges to a District Court's guideline determinations, this Court reviews "the district court's interpretation of the Sentencing Guidelines *de novo* . . . and reviews the district court's findings of fact for clear error." *United States* v. *Rubenstein*, 403 F.3d 93, 99 (2d Cir. 2005) (citations omitted).

In addition to ensuring that the sentencing was procedurally proper, this Court reviews sentences for substantive reasonableness. *United States* v. *Crosby*, 397 F.3d 103, 114-15 (2d Cir. 2005). "[R]easonableness review does not entail the substitution of [the Court's] judgment for that of the sentencing judge. Rather, the standard is akin to review for abuse of discretion." *United States* v. *Fernandez*, 443 F.3d 19, 27 (2d Cir. 2006). "[I]n the overwhelming majority of cases, a Guidelines sentence will fall comfortably within the broad range of sentences that would be reasonable in the particular circumstances." *Id.* at 33.

B. The Loss Calculation Was Correct

1. Applicable Law

Section 2B1.1(b)(1) of the Sentencing Guidelines specifies upward enhancements depending on, among other things, the amount of actual or intended loss. Although there was no actual loss, Aleynikov's crime carried a substantial "intended loss" — pecuniary harm "that was intended to result from the offense." U.S.S.G. § 2B1.1 cmt. 3(A) ("Intended loss" even includes "harm that would have been impossible or unlikely to occur.").

The Guidelines provide a non-exhaustive list of factors that can be used to estimate the loss amount:

(i) The fair market value of the property unlawfully taken, copied, or destroyed; or, if the fair market value is impracticable to determine or inadequately measures the harm, the cost to the victim of replacing that property.

(ii) In the case of proprietary information (e.g., trade secrets), the cost of developing that information or the reduction in the value of that information that resulted from the offense.

* * *

(vi) More general factors, such as the scope and duration of the offense and revenues generated by similar operations.

U.S.S.G. § 2B1.1 cmt. 3(C).

"In calculating the amount of loss under the Guidelines, a sentencing court 'need only make a reasonable estimate of the loss.'" *United States* v. *Rigas*, 583 F.3d 108, 120 (2d Cir. 2009) (quoting U.S.S.G. § 2B1.1 cmt. 3(C)). Although determining the loss amount may be "no easy task[,] . . . some estimate must be made for Guidelines' [calculation] purposes, or perpetrators of fraud would get a windfall." *United States* v. *Rigas*, 583 F.3d at 120 (citations and quotations omitted)).

Loss amount must be established by a preponderance of the evidence and is subject to review only for clear error. *See United States* v. *Brennan*, 395 F.3d 59, 74 (2d Cir. 2005). "The sentencing judge is in a unique position to assess the evidence and estimate the loss based upon

that evidence." U.S.S.G. § 2B1.1 cmt. 3(C). "When making sentencing determinations, a district court may rely on any facts available to it, . . . [including] circumstantial evidence and on reasonable inferences drawn therefrom. Indeed, this will often have to be the case when the issue in dispute is a defendant's knowledge and intent." *United States* v. *Gaskin*, 364 F.3d at 464.

2. Relevant Facts

The evidence before the District Court relating to loss included:

- Goldman initially purchased its trading system Hull for $500 million. (A. 556).
- Goldman generated at least $300 million in net pretax income in 1999 using HFT. (A. 556).
- The 25 computer programmers in Aleynikov's group were collectively paid approximately $6.8 million per year. (A. 556).
- The cost of the expensive commercially-available components, including one called "Wombat," that perform the same functions as some of the components stolen by Aleynikov. (A. 566; Tr. 539-41).
- To develop an HFT system from scratch would take two years and $10 million. (A. 556; Tr. 701-703).

Judge Cote conducted a thorough review of the record and determined a "7 to $20 million loss figure" to be "amply supported" by evidence from the trial, and found that, "[i]f anything, the loss figure is close to or exceeds

$20 million." (A. 559). In addition to reviewing the above evidence, Judge Cote also found that it would take 25 programmers approximately 2 to 3 years to write 500,000 lines of source code (the approximate amount of code the defendant stole) at a cost of between $14 million and $21 million. (A. 559). Judge Cote also rejected Aleynikov's argument that he did not intend to cause economic harm Goldman, finding that the jury had rejected that defense and that, in any event, given that Goldman is purely in "business to make money, " "[i]t is difficult to imagine what other harm or injury Aleynikov could have caused Goldman in taking its proprietary code." (A. 559). The District Court also rejected Aleynikov's argument that the loss amount grossly overstated the extent of his theft, finding that Aleynikov's "intent . . . was to steal massive amounts of extraordinarily valuable proprietary source code . . . knowing full well that he would be inflicting a terrible blow to Goldman and its expensive effort to build a superior [HFT] system." (A. 559).

3. Discussion

Despite having conceded that the stolen code has value (A. 557-58), Aleynikov continues to contend that there is "no evidence to support any intended loss." (Br. 54). Aleynikov's arguments fail to demonstrate, however, that the District Court clearly erred in arriving at its loss calculation, which is amply supported by the record evidence.

Aleynikov incorrectly claims that "district court focused on three facts" to support its loss calculation — the Hull acquisition, the revenue generated by the system, and the salaries paid to Goldman programmers. (Br. 54-

55). These facts amply supported the finding, but these were not the only facts Judge Cote considered. For example, Aleynikov completely ignores the District Court's calculation of the development cost of writing all 500,000 lines of stolen source code. (A. 559). This calculation alone supports the District Court's loss calculation.*

Aleynikov incorrectly claims that "it was undisputed that the code Aleynikov downloaded contained *substantial* open source material" (*Id*. (emphasis added)), and argues that this should have reduced the loss amount. To the contrary, this claim was very much disputed and is contrary to the trial evidence. (*See*, *e.g.*, Tr. 1531-36). Indeed, even Aleynikov's expert testified that the "vast majority" of the files compressed within one of the stolen tarball files bore Goldman copyright notices, and that he only identified one file that bore a Goldman copyright but contained open source code. (Tr. 1367, 1428-29).

Aleynikov argues that there was "no evidence" that showed how many of the group of 25 Goldman programmers worked on the stolen code. (Br. 56). But Aleynikov ignores the evidence that this group (and others at Goldman) continually writes and maintains code for

---

* Aleynikov's reliance on *United States* v. *Dickler*, 64 F.3d 818 (3d Cir. 1995), to argue that the factors in U.S.S.G. § 2B1.1 cmt. 3(C) "do not apply" (Br. 54), is misplaced because the District Court properly found an intended loss. By contrast, *Dickler* involved a crime with no intended or actual loss. *United States* v. *Dickler*, 64 F.3d at 826.

Goldman's HFT system, including the components stolen by Aleynikov. (Tr. 345-46, 449-52, 480-93, 977-78).

Further, Aleynikov falls back on his argument that he lacked the intent to harm Goldman (and therefore there was no intended loss), which is addressed *supra*, and which was necessarily rejected by the jury in returning a guilty verdict under the EEA.

Finally, Aleynikov asserts that he could not effectively contest the loss amount at sentencing because his pretrial request to obtain a copy of Goldman's entire trading platform was denied by the District Court. (SPA 115-22). However, Aleynikov does not challenge the discovery ruling on appeal, nor does his conclusory assertion explain how the ruling bears on the loss calculation.

C. Agrawal's Sentence Did Not Require a Below-Guidelines Sentence

1. Applicable Law

Although under 18 U.S.C. § 3553(a)(6), district courts are required to consider "the need to avoid unwarranted sentence disparities," this Court has held that a sentencing disparity is not unwarranted unless the defendants are similarly situated. *See United States* v. *Fernandez*, 443 F.3d 19, 31-32 (2d Cir. 2006).

Moreover, the requirement that a sentencing judge consider any of the 18 U.S.C. § 3553(a) factors "is *not* synonymous with a requirement that the factor be given determinative or dispositive weight in the particular case, inasmuch as it is only one of several factors that must be weighted and balanced by the sentencing judge." *United*

States v. *Fernandez*, 443 F.3d at 32 (emphasis in original); *United States* v. *Florez*, 447 F.3d 145, 157-58 (2d Cir. 2006) (the weight to be given to any sentencing disparities "like the weight to be given any § 3553(a) factor, is a matter firmly committed to the discretion of the sentencing judge" (internal quotation marks omitted)).

2. Discussion

At sentencing, Aleynikov argued for a non-Guidelines sentence, in part, based on the non-Guidelines sentence imposed in *Agrawal*. Aleynikov noted that, among other things, Judge Rakoff found that the loss amount in *Agrawal* (which was also between $7 million and $20 million) resulted in a Guidelines range (63 to 78 months' imprisonment) that was more than necessary to meet the sentencing goals of Section 3553(a). (A. 566).

Judge Cote carefully reviewed *Agrawal* and noted several differences between Agrawal and Aleynikov, such as (i) Agrawal's "genuine acceptance of responsibility"; (ii) that in *Agrawal* the sophisticated means enhancement was not applicable; (iii) that Judge Rakoff found that "[t]here was no need for specific deterrence"; (iv) that Judge Rakoff also found that Agrawal was "someone who in the course of his life had shown considerable generosity and breadth of spirit who was essentially a good guy"; and (v) that Agrawal faced "the possibility of deportation." (A. 568). Furthermore, Judge Cote noted that unlike in *Agrawal*, the loss amount in the instant case did not have an "inappropriate impact on the sentence." (*Id.*)

Judge Cote also addressed, at length, her reasons for rejected Aleynikov's remaining arguments and imposing

the sentence she did. (A. 567-68). Judge Cote found that specific deterrence was a significant issue because of Aleynikov's lack of remorse; his attempt to shift blame to the victim and to the Government; his past misappropriation of intellectual property; and his awareness that he did not have permission to remove any code from Goldman. (A. 569).

> [T]his conduct that the defendant engaged in deserves a significant sentence because the scale of his theft was audacious. The value of the property taken was extremely high. He took months to plan and execute the crime. It was motivated solely by greed, and it was characterized by supreme disloyalty to his employer.

(A. 569).

Thus, the District Court did not "ignore" the sentence in *Agrawal* (Br. 10), but instead carefully considered and distinguished that case. (A. 568). The District Court also addressed, at length and in detail, its reasons for imposing the sentence in this case under Section 3553(a). (A. 567-69). Accordingly, the District Court's sentence was reasonable. *See United States* v. *Florez*, 447 F.3d at 157-58 (the weight to be given to any sentencing disparities "like the weight to be given any § 3553(a) factor, 'is a matter firmly committed to the discretion of the sentencing judge'").

CONCLUSION

The judgment of conviction should be affirmed.

Dated: New York, New York
September 6, 2011

Respectfully submitted,

PREET BHARARA,
United States Attorney for the Southern District of New York, Attorney for the United States of America.

JOSEPH P. FACCIPONTI,
JUSTIN S. WEDDLE,
Assistant United States Attorneys, Of Counsel.

CERTIFICATE OF COMPLIANCE

Pursuant to Rule 32(a)(7)(C) of the Federal Rules of Appellate Procedure, the undersigned counsel hereby certifies that this brief complies with the type-volume limitation of Rule 32(a)(7)(B). As measured by the word-processing system used to prepare this brief, there are 13,999 words in this brief.

PREET BHARARA,
United States Attorney for the
Southern District of New York

By: JUSTIN S. WEDDLE,
Assistant United States Attorney